What Is Claimed Is:

1   1.   A method for detecting a denial-of-service attack using an

2   execution profile for a kernel of a server computer system, comprising:

3   producing a run-time execution profile by gathering statistics related to

4   execution of a protocol stack within the kernel of the server;

5   wherein the protocol stack processes packets received from client

6   computer systems;

7   comparing the run-time execution profile with a normal execution profile

8   for the kernel of the server;

9   wherein the normal execution profile is representative of execution when

10   the server is not subject to a denial-of-service attack; and

11   indicating that a denial-of-service attack is taking place if the run-time

12   execution profile deviates from the normal execution profile.

1   2.   The method of claim 1, wherein producing the run-time execution

2   profile involves gathering statistics regarding a fraction of time that the server

3   spends executing one or more portions code related to the protocol stack.

1   3.   The method of claim 2, wherein producing the run-time execution

2   profile involves producing a vector indicating a number of times that the server is

3   found to be executing the one or more portions of code related to the protocol

4   stack.

1   4.   The method of claim 2, wherein the one or more portions of code

2   related to the protocol stack include:

3   a portion related to processing TCP SYN requests;

4   a portion related to processing TCP ACKs;

5   a portion related to processing TCP data;

6   a portion related to processing ICMP echo requests; and

7   a portion that is unrelated to the protocol stack.

1   5.   The method of claim 1, further comprising producing the normal

2 execution profile by gathering statistics related to execution of the server when the

3 server is not subject to a denial-of-service attack.

1   6.   The method of claim 1, wherein if a denial-of-service attack is

2 detected, the method further comprises blocking offending packets from reaching

3 the server.

1   7.   The method of claim 1, wherein producing the run-time execution

2 profile involves gathering statistics over a first time window, and subsequently

3 gathering statistics for a subsequent run-time execution profile over a second time

4 window.

1   8.   The method of claim 7, further comprising gathering statistics for a

2 concurrent execution profile over a concurrent time window that overlaps the first

3 time window and the second time window, so that a denial-of service attack that

4 overlaps the first time window and the second time window can be detected in the

5 concurrent time window.

1   9.   The method of claim 1, wherein comparing the run-time execution

2 profile with the normal execution profile involves determining if the run-time

13

3 execution profile deviates more than a pre-specified amount from the normal

4 execution profile.

1   10.   A computer-readable storage medium storing instructions that

2 when executed by a computer cause the computer to perform a method for

3 detecting a denial-of-service attack using an execution profile for a kernel of a

4 server computer system, the method comprising:

5   producing a run-time execution profile by gathering statistics related to

6 execution of a protocol stack within the kernel of the server;

7   wherein the protocol stack processes packets received from client

8 computer systems;

9   comparing the run-time execution profile with a normal execution profile

10 for the kernel of the server;

11   wherein the normal execution profile is representative of execution when

12 the server is not subject to a denial-of-service attack; and

13   indicating that a denial-of-service attack is taking place if the run-time

14 execution profile deviates from the normal execution profile.

1   11.   The computer-readable storage medium of claim 10, wherein

2 producing the run-time execution profile involves gathering statistics regarding a

3 fraction of time that the server spends executing one or more portions code related

4 to the protocol stack.

1   12.   The computer-readable storage medium of claim 11, wherein

2 producing the run-time execution profile involves producing a vector indicating a

3 number of times that the server is found to be executing the one or more portions

4 of code related to the protocol stack.

14

1   13.   The computer-readable storage medium of claim 11, wherein the

2   one or more portions of code related to the protocol stack include:

3   a portion related to processing TCP SYN requests;

4   a portion related to processing TCP ACKs;

5   a portion related to processing TCP data;

6   a portion related to processing ICMP echo requests; and

7   a portion that is unrelated to the protocol stack.

1   14.   The computer-readable storage medium of claim 10, wherein the

2   method further comprises producing the normal execution profile by gathering

3   statistics related to execution of the server when the server is not subject to a

4   denial-of-service attack.

1   15.   The computer-readable storage medium of claim 10, wherein if a

2   denial-of-service attack is detected, the method further comprises blocking

3   offending packets from reaching the server.

1   16.   The computer-readable storage medium of claim 10, wherein

2   producing the run-time execution profile involves gathering statistics over a first

3   time window, and subsequently gathering statistics for a subsequent run-time

4   execution profile over a second time window.

1   17.   The computer-readable storage medium of claim 16, wherein the

2   method further comprises gathering statistics for a concurrent execution profile

3   over a concurrent time window that overlaps the first time window and the second

15

4   time window, so that a denial-of service attack that overlaps the first time window

5   and the second time window can be detected in the concurrent time window.

1   18.   The computer-readable storage medium of claim 10, wherein

2   comparing the run-time execution profile with the normal execution profile

3   involves determining if the run-time execution profile deviates more than a pre-

4   specified amount from the normal execution profile.

1   19.   A apparatus that detects a denial-of-service attack through use of

2   an execution profile for a kernel of a server computer system, comprising:

3   a profiling mechanism that is configured to produce a run-time execution

4   profile by gathering statistics related to execution of a protocol stack within the

5   kernel of the server;

6   wherein the protocol stack processes packets received from client

7   computer systems;

8   a comparison mechanism that is configured to compare the run-time

9   execution profile with a normal execution profile for the kernel of the server;

10   wherein the normal execution profile is representative of execution when

11   the server is not subject to a denial-of-service attack; and

12   wherein the comparison mechanism is configured to indicate that a denial-

13   of-service attack is taking place if the run-time execution profile deviates from the

14   normal execution profile.

1   20.   The apparatus of claim 19, wherein the profiling mechanism is

2   configured to gather statistics regarding a fraction of time that the server spends

3   executing one or more portions code related to the protocol stack.

16

1   21.   The apparatus of claim 20, wherein the profiling mechanism is

2   configured to produce a vector indicating a number of times that the server is

3   found to be executing the one or more portions of code related to the protocol

4   stack.

1   22.   The apparatus of claim 20, wherein the one or more portions of

2   code related to the protocol stack include:

3   a portion related to processing TCP SYN requests;

4   a portion related to processing TCP ACKs;

5   a portion related to processing TCP data;

6   a portion related to processing ICMP echo requests; and

7   a portion that is unrelated to the protocol stack.

1   23.   The apparatus of claim 19, wherein the profiling mechanism is

2   additionally configured to produce the normal execution profile by gathering

3   statistics related to execution of the server when the server is not subject to a

4   denial-of-service attack.

1   24.   The apparatus of claim 19, further comprising a blocking

2   mechanism that is configured to block offending packets from reaching the server

3   if a denial-of-service attack is detected.

1   25.   The apparatus of claim 19, wherein while producing the run-time

2   execution profile, the profiling mechanism is configured to gather statistics over a

3   first time window, and to subsequently gather statistics for a subsequent run-time

4   execution profile over a second time window.

1 26. The apparatus of claim 25, wherein the profiling mechanism is
2 additionally configured to gather statistics for a concurrent execution profile over
3 a concurrent time window that overlaps the first time window and the second time
4 window, so that a denial-of service attack that overlaps the first time window and
5 the second time window can be detected in the concurrent time window.

1 27. The apparatus of claim 19, wherein the comparison mechanism is
2 configured to determine if the run-time execution profile deviates more than a pre-
3 specified amount from the normal execution profile.

18